Hierarchal Trust Certificate Distribution using Distributed CA in MANET

V. Vinoth Kumar, K. S. Arvind, S. Umamaheswaran, Suganya K.S

Abstract: ***In the growing network generation of wireless systems, there is a necessity usage of deploying wireless network for usage of individual mobile users. The considerable examples are the deploying MANET in emergency situations like disaster, military surveillance, tactical networks, data networks etc. This network situation doesn't work on centralized and adopt the rely operations without access points. All these application areas adopts infrastructure less environment which facilitates highly possible network attacks. Identifying such a security breach happening in network would be a Herculean task. This research identifies trusted parties will involve in message communication and provides privacy of the message being sent to destination using cryptographic mechanisms. When two or more networks involve in data communication at that situation making the authentication with the help of certification distribution method would be a difficult task. Hence the nodes are dropping the packet or unauthorized parties do the denial of service so that delay will increase and throughput is reduced. In order to overcome this issue, the cross certification method is implemented with the distribution of certificate using hierarchal trust. This method solves the issue of authentication problem and coordinates for all the nodes to communicate to each other as a trusted party. When two ad hoc networks merge, we need a mechanisms for nodes originated from different networks to certify and authenticate each other. Finally the simulation was conducted with certain parameters and achieved better throughput and reduced delay of data transfer.***

Keywords: Digital Certificate, trust model, TLS, MANET, AODV

I. INTRODUCTION

In Ad hoc Network, Ad hoc On-Demand Distance Vector (AODV) protocol category of re-active routing protocol and it gives better performance through the on demand connection establishment. The improvement of this type of routing protocol is that it maintains routing information and updates every route establishment. It provides more flexibility on network deployment and supports both unicast and multicast routing. Security in MANET is a more important need and many researches are going on to solve the attacks and provide trust. Generally the Public key cryptography and private key cryptography methods are using to provide the security and avoid the vulnerabilities. These two crypto systems approaches use different algorithms and protocols to enhance security. For internet based applications the security aspects implemented by the way of layered mechanism like Transport Layer Security (TLS), PGP, and GPG. The further level of security implementations on next generation's wireless network is to distribute the authorization between nodes called as certificate. This certificate will be distributed by certificate authority (CA) likely to be a third party of the network. However this distribution of certificate is not improved security on the network due to adaptation on trust models. Different trust models following various method of passing certificate between nodes for achieving better results. Some trust models adopt for standard network like internet based but it may not suitable for wireless network. In order to manage the certificate, trust agent uses the certificate repository and maintain with the unique id. But every repository has certain limitations and drawback to maintain their certificates. In order to follow the sequence of certificate distribution chain management schemes are used. Key authentication is also performed through chains of certificates.

Manuscript published on 30 August 2019.

*****Correspondence Author(s)
Dr.V.Vinoth Kumar*, Associate Professor, Department of Computer Science & Engineering, MVJ College of Engineering, Bangalore, India,
Dr.K.S.Arvind, Associate Professor, Department of Computer Science & Engineering, MVJ College of Engineering, Bangalore, India,
Dr.S.Umamaheswaran, Associate Professor, Department of Computer Science & Engineering, MVJ College of Engineering, Bangalore, India,
K.S.Suganya, Assistant Professor, Department of Information Technology, Bannari Amman Institute of Technology, India,

II. RELATED WORK

The Trusted Third Party (TTP) used for distribution of certificates between mobile nodes. This category is based on special PKI servers, digital certificate, Kerberos and exchange of key pairs. Hence this scheme used partial digital signature and public key certificate for implementing trusted data exchange [1]. The distribution of certificate depends on threshold cryptography and functionality characteristics of network nodes. However the overheads are increasing during data exchange on unreliable network. This overhead challenge could be reduced using cache routes and parallel maintaining repository servers [2]. The Distributed Certification Authority with probabilistic freshness for ad hoc networks (DICTATE) scheme focus on identity based crypto systems for providing security on ad hoc network. It invokes the certification distribution method using grouping the characteristics of relying nodes and ensures the certificate update request [3]. An ID-based Key Management system with public keys provides security for SSL based applications. It eliminates individual certificate needs of every nodes present on the network. This novel method also focuses on public key management scheme and identity based private key distribution [4]. An elucidation of a distributed Certificate Authority based on levels of key exchange and key management.

Retrieval Number: J95600881019/19©BEIESP
DOI: 10.35940/ijitee.J9560.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

This scheme follows the idea of implementing distribution of certificate through node degree, number of adjacent nodes and service delays. Hence, the solution can be vary depends on dynamically varying the values of threshold [5].

The scheme of CA distribution for cluster based architecture. In each cluster, the cluster head liable to maintain information about CA in their table. So each table maintains the detail about number of nodes present, neighbor node, energy level etc. Thus the distributed CA maintains details about all the group heads and it reduces the end to end and control overhead [6]. Certificate based key management system uses public keys for distribution of central CA. The trusted CA deals all the keys involved in the key management system for improving security by the way of authentication. Thus the system works for authentication along with revocation, updating [7]. Thus the cryptographic solutions for infrastructure less network like MANET used for real time applications. As per the result every node distributes public key certificates for its domain and authenticates chain of trust. Every node holds more than one certificate as possible to make a multicast communication. The distributed clustering follow the CA based routing between each local cluster. It focuses on security aspects for self organized networks and public key based certificates. The certificates are lined as a chain to transfer from one cluster to another cluster [8, 9].

III. PROPOSED METHODOLOGY

In a proposed system follows the hierarchical structure and it has root node called as Certificate Authority (CA). The trust extends from the CA and reaches to last node through intermediate nodes. This distribution goes down as a chain and gets back the certificate acknowledgement by root node.

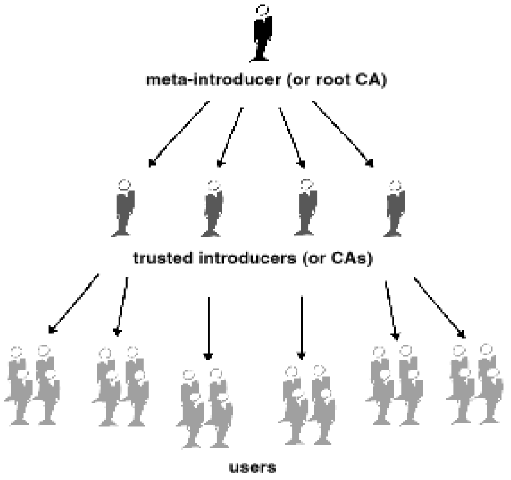


Fig.1 Hierarchical trust

In a Fig.1, the certificate distribution follows hierarchical Trust model. This model has two types of methods as Certificate issuance and Certificate Revocation.

A. *Certificate Issuing/Renewal:*

The certificate Issuing method follows distribution scheme and multi-signature scheme. In the distribution scheme adopt algorithm and shown as fig 2.

B. *Certificate Revocation:*

When the communication has been ended between trusted parties, there is necessary situation to revocation of certificates. Each trust is created and maintained between mobile node and neighbor node. It helps to each node participate the network activity and transfer the secure data. All the transaction will get the ACK for reliability.

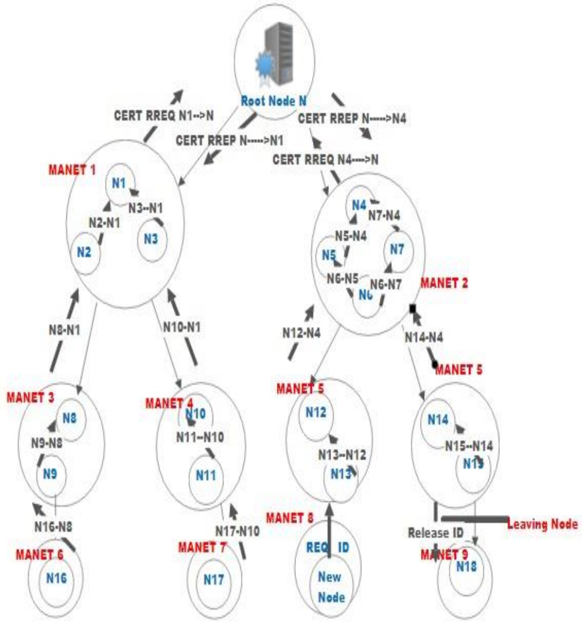


Fig.2 Certificate distribution Method in Hierarchal Trust

C. *Algorithm For certificate distribution in hierarchal trust :*

```
Procedure
Root N→ CA
Initialize: node N = first node of the level 1
If N > maximum hash value
for each peer i do for all levels,
Node N+1 initiate a request to its predecessor N
N finds the trust value ($T_v$) for N+1
if $T_v$ > 1 then
N+1 Receive the $CERT_{vi}$ from N
node N+1 finds the node on next level,
for all received certificate pair ($CERT_{vi}$; j), where j is an
next pair $CERT_{vj}$
Receive the overall status vj from the central manager of
node j
```

D. *Distributed CA*

In RSA algorithm, the CA shares two types of keys named as Private Key (pkCA) and shared key (skCA). Bothe the keys are used for distribution of key between nodes among N nodes. Each node shares the CA with the polynomial equation of Si = f(i) mod N. Hence, least k sends the high limit and it can be evaluated by using Eq. (1),

$$f(x) = \sum_{i=1}^{k} S x_i .li(x) mod\ N \tag{1}$$

Where $li(x)$ is the coefficient

Hence the encryption and message digest methods follows partial operation on distribution of certificate in below mentioned equation Eq. (2),

$$Sign\ i = digest\ Sx_i \bmod N \qquad (2)$$

The polynomial secret key (SK) has distributing among the network nodes. In our proposed algorithms, each node vi's polynomial distributes P_{vi} and its complement share SK_{vj} in term of a the new certificate $CERT_{vi}$ to generate by the below equation as,

$$CERT_{vi} = (cert)\, SK_{vj} \bmod N \qquad (3)$$

Node v_j sends $CERT_{vj}$ to the requesting node v_i .

E. *Join and Leaving of nodes*

Each node n included in the network and few keys before allotted to n's successor and it assigned to n.

Pseudo code for finding neighbor node to join:

```
// Finding the neighbor node N
Intial id= 0 ,n.
n.find (neighbor id)
    if (id ∈ (current id,n, neighbor id)
        return neighbor id;
    else
        // broadcast the request to the MANET
        return successor_id;
        find_successor(id);
```

Node 'n' removed from the network, the following operations will occur as, all the keys are again assigned to n's successor. Identify the id of the leaving node among all nodes using pointers. If the node found with their id, send the request for withdraw as certificate revocation. Once the node returns their certificate next the trust relation automatically breaks. If it has failed, the node already breaks the authentication and no need to withdraw certificate.

IV. RESULTS AND DISCUSSION

The RSA algorithm has been implemented for key generation and MD5 has been used for as the encryption technique for the message transfer. NS2 is used to analyzing and simulate the performance results. The input files are rsa.tcl and mdpure.tcl files in which the simulation parameters are specified. The simulation parameter values are shown below on Table I.

Table –I: Experimental Setup

Param.	Value
Routing Protocol	AODV
Transmission Rate	2 Mbps
Simulation Duration	70 seconds
MAC	802.11
Mobility	RWP
No. of nodes	50
Node speed	3 m/s
Queue length	1500
Pause time	0, 30s
Queue type	DropTail/PriQueue
Network Area	800 m X 1000m
Traffic	CBR
System Specification	VM ware and ubuntu, 1Gb Ram and 20 Gb Harddisk

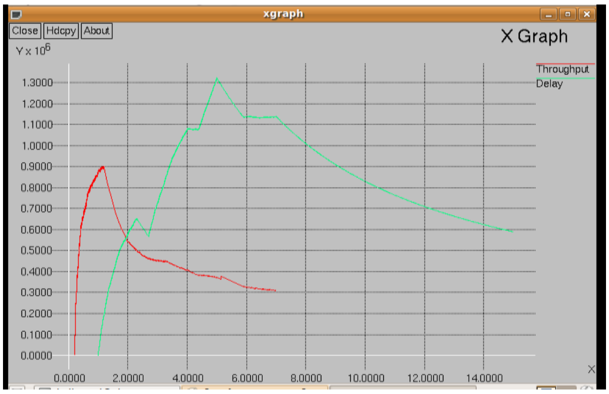
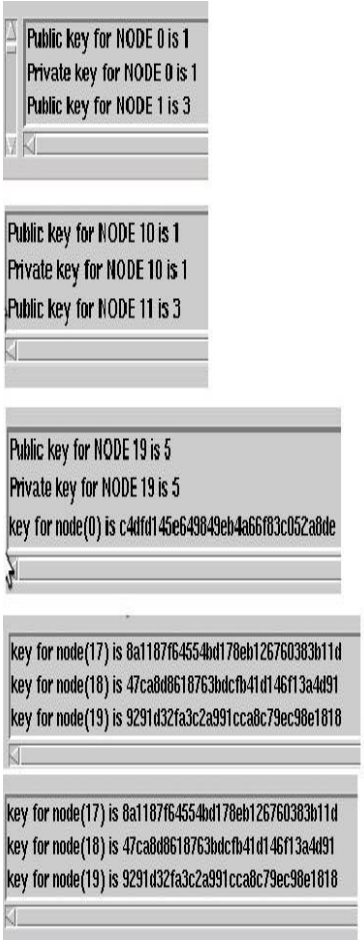


Fig.3 Throughput Vs Delay

The capacity shows the throughput value of the complete system with all nodes, and the delay shows the average time of a packet transmitting from source to destination in the network. In fig.3 the graph shows that we had increased the throughput and kept the delay in some threshold value while achieving the node authentication and data integrity.



```
Public key for NODE 0 is 1
Private key for NODE 0 is 1
Public key for NODE 1 is 3
```

```
Public key for NODE 10 is 1
Private key for NODE 10 is 1
Public key for NODE 11 is 3
```

```
Public key for NODE 19 is 5
Private key for NODE 19 is 5
key for node(0) is c4dfd145e649849eb4a66f83c052a8de
```

```
key for node(17) is 8a1187f64554bd178eb126760383b11d
key for node(18) is 47ca8d8618763bdcfb41d146f13a4d91
key for node(19) is 9291d32fa3c2a991cca8c79ec98e1818
```

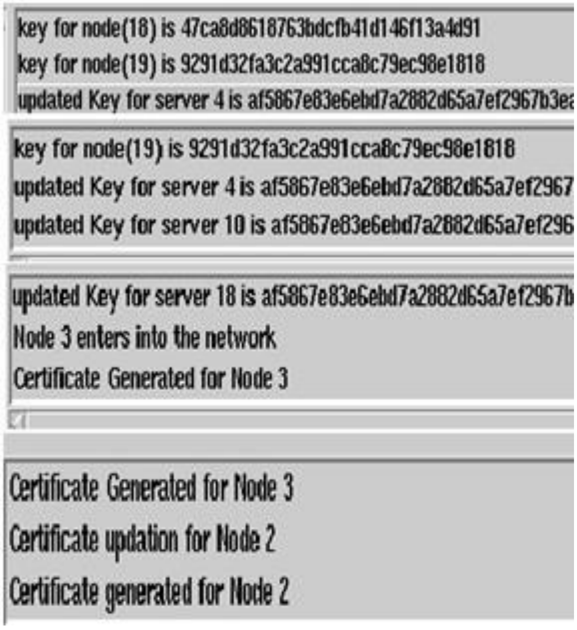
```
key for node(17) is 8a1187f64554bd178eb126760383b11d
key for node(18) is 47ca8d8618763bdcfb41d146f13a4d91
key for node(19) is 9291d32fa3c2a991cca8c79ec98e1818
```

Fig .4 Key assignments and certificate generation

In Fig. 4 shows the key assigning for each node in the network and the certificate generation for each node.

Retrieval Number: J95600881019/19©BEIESP
DOI: 10.35940/ijitee.J9560.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)



```
key for node(18) is 47ca8d8618763bdcfb41d146f13a4d91
key for node(19) is 9291d32fa3c2a991cca8c79ec98e1818
updated Key for server 4 is af5867e83e6ebd7a2882d65a7ef2967b3ea

key for node(19) is 9291d32fa3c2a991cca8c79ec98e1818
updated Key for server 4 is af5867e83e6ebd7a2882d65a7ef2967
updated Key for server 10 is af5867e83e6ebd7a2882d65a7ef296

updated Key for server 18 is af5867e83e6ebd7a2882d65a7ef2967b
Node 3 enters into the network
Certificate Generated for Node 3

Certificate Generated for Node 3
Certificate updation for Node 2
Certificate generated for Node 2
```

Fig.5 Key updation and certificate generation for new node

In fig 5 shown that when there is any packet dropping and any attacks in the network the key updation is done in order to maintain the security. As the MANET is a transient mobile network there will be node movement when new node joins in the network certificates have been generated according to the key provided by those nodes.

V. CONCLUSION

The Public key authentication scheme in mobile ad hoc networks allows secured communication between the nodes and the existence of web between trusted nodes. This scheme allows a users need to create their public key as well as equivalent private key, to distribute certificates to neighboring nodes, for the establishment of trust relationship between the nodes which involve in the communication and to perform public key authentication without sending to centralized authority. The certificate chain discovery performs during the routing process. This discovery of certificate chain provides the successful secured communication between the trusted nodes.

REFERENCES

1. L. Zhou and Z. J. Haas, “Securing ad hoc networks,” *IEEE Network*, vol. 13, no. 6, pp. 24–30, 1999.
2. S. Yi and R. Kravets, “MOCA: mobile certificate authority for wireless ad-hoc networks,” in *Proceedings of the 2nd Annual PKI Research Workshop* (PKI '03), 2003.
3. R. Li, J. Li, P. Liu, and H.-H. Chen, “On-demand public-key management for mobile ad hoc networks,” *Wireless Communications and Mobile Computing*, vol. 6, no. 3, pp. 295–306, 2006.
4. .Y. Zhang, W. Liu, W. Lou, and Y. Fang, “Securing mobile ad hoc networks with certificateless public keys,” *IEEE Transactions on Dependable and Secure Computing*, vol. 3, no. 4, pp. 386–399, 2006.
5. S. Raghani, D. Toshniwal, and R. Joshi, “Dynamic support for distributed certification authority in mobile ad hoc networks,” *in Proceedings of the International Conference on Hybrid Information Technology* (ICHIT '06), pp. 424–432, November 2006.
6. Y. Dong, A.-F. Sui, S. M. Yiu, V. O. K. Li, and L. C. K. Hui, “Providing distributed certificate authority service in cluster-based mobile ad hoc networks,” *Computer Communications*, vol. 30, no. 11-12, pp. 2442–2452, 2007.
7. S. Kent, Privacy enhancement for Internet electronic mail: Part II: Certi_cate-based key management, Tech. rep., *Network Working Group, request for Comments*: 142 (1993).
8. S. Capkun, L. Buttyan, and J.-P. Hubaux, “Self-organized public-key management for mobile ad hoc networks,” *IEEE Transactions on Mobile Computing*, vol. 2, no. 1, pp. 52–64, 2003.
9. K. Ren, T. Li, Z. Wan, F. Bao, R. H. Deng, and K. Kim, “Highly reliable trust establishment scheme in ad hoc networks,” *Computer Networks*, vol. 45, no. 6, pp. 687–699, 2004.

AUTHORS PROFILE

Dr. V. Vinoth Kumar is an Associate Professor in the Department of Computer Science and Engineering at MVJ College of Engineering, Bangalore, India. He is a highly qualified individual with around 8 years of rich expertise in teaching, entrepreneurship, and research and development with specialization in computer science engineering subjects. He has been a part of various seminars, paper presentations, research paper reviews, and conferences as a convener and a session chair, a guest editor in journals and has co-authored several books and papers in national, international journals and conferences. He is a professional society member for ISTE, IACIST and IAENG. He published more than 15 articles in National and International journals, 10 articles in conference proceedings and one article in book chapter. His Research interest includes Mobile Adhoc Networking and IoT.

Dr. K. S. Arvind was born in Salem, Tamilnadu, India. He completed his undergraduate in Computer Science and Engineering at Pondicherry University, India.Then, he received his postgraduate in Computer Science and Engineering at Anna University, Chennai, India. He had completed a Ph.D. in Computer Science and Engineering at Anna University, Chennai, India from 2006-2007, he worked as a Software engineer in Application testing with Signy Technologies, Pondicherry. Currently, he is working with MVJ College of Engineering as an Associate Professor. He is the author of many articles published in International & National. He also holds memberships in IEEE, IACSIT and CSTA. His areas of interest include Cloud Security and Privacy.

Dr. S. Umamaheswaran is currently working as Associate Professor in the Department of Computer Science and Engineering at M V J College of Engineering, Bangalore, India. He holds a Bachelor’s degree in Mathematics, a Master’s degree in Computer Applications from Madurai Kamarajar University, Madurai, a Master’s degree in Computer Science and Engineering from National Engineering College, Kovilpatti, India. He completed his doctoral degree at Anna University, Chennai, India. His research interests include Image processing, Decision Support System and Big Data.

K. S. Suganya had completed Under-graduation and Post-graduation from Anna University and perusing Research from Anna University, Chennai. She had started her career as a Programmer Analyst in Cognizant Technology Solutions and currently associated with Bannari Amman Institute of Technology as Assistant Professor. Her area of interest is Blockchain Technology, Internet of Things and Security.